CLAIMS:

1. A method of providing and authenticating secure data over a network, comprising:

establishing a first secure connection from a user device to a first server;

encrypting an enrollment request with a first authentication key, and thereafter sending the encrypted enrollment request to a host application;

encrypting an enrollment applet, a public key and signed data with the first authentication key and thereafter returning the encrypted enrollment applet, public key and signed data from the host application to the first server;

decrypting the enrollment applet and sending the enrollment applet from the first server to the user device using the first secure connection;

establishing a second secure connection from the user device to a second server;

encrypting the secure data with the public key using the enrollment applet;

linking the signed data and the encrypted secure data and thereafter sending the linked data to the second server;

encrypting the linked data with a second authentication key and sending the encrypted linked data to the host application;

verifying the signed data and thereafter creating authentication data;

encrypting the authentication data and the secure data and sending the encrypted authentication data and secure data to the second server;

storing the encrypted authentication data and the secure data.

2. The method of claim 1, wherein the signed data comprises a serial number and an account number.

3. The method of claim 1, further comprising exchanging the first authentication key between the first server and the host application and exchanging the second authentication key between the second server and the host application.

4. The method of claim 1, wherein storing the encrypted authentication data and the secure data includes storing at least a portion of the authentication data and the secure data in the enrollment applet.

5. The method of claim 1, wherein storing the encrypted authentication data and the secure data includes storing at least a portion of the authentication data and the secure data in a mobile storage medium.

6. The method of claim 5, wherein the mobile storage medium is a smart card device which may be used to access an account from at least one remote location.

7. A method of providing and authenticating secret data over a network, the network comprising a user device, a first server, a second server and a host application, comprising: establishing a first secure connection between the user device and the first server in response to an enrollment request from a user;

sending encrypted enrollment information from the host application to the first server;

decrypting the enrollment information at the first server;

sending an enrollment applet and a unique identifier from the first server to the user device, the unique identifier identifies the user device;

establishing a second secure connection between the user device and the second server;

encrypting an access code using the customer applet;

linking the encrypted access code with the unique identifier and thereafter sending the linked encrypted access code and the unique identifier to the second server;

encrypting the linked data at the second server and thereafter sending the encrypted linked data to the host application;

verifying the unique identifier at the host application and thereafter creating authentication data;

encrypting the authentication data with the access code;

sending the encrypted authentication data and access code from the host application to the second server;

sending the encrypted authentication data and access code from the second server to the customer applet using the second secure connection; and

storing the encrypted authentication data and access code in the customer applet.

8. The method of claim 7, wherein the access code is a personal identification number (PIN).

9. The method of claim 7, wherein the access code is a password.

10. The method of claim 7, wherein storing the encrypted authentication data and access code includes storing at least a portion of the encrypted authentication data and the access code in the customer applet.

11. The method of claim 10, further comprising:

encrypting and sending an enrollment applet, a public key, a serial number and an account number from the host to the first server; and

decrypting the enrollment applet, a public key, a serial number and an account number at the first server.

12. The method of claim 7, wherein storing the encrypted authentication data and access code includes storing at least a portion of the encrypted authentication data and the access code on a mobile storage medium.

13. The method of claim 12, wherein the mobile storage medium is a smart card device which may be used to access an account from at least one remote location.

14. A method of providing and authenticating an access code, comprising:

establishing a first secure connection from a user to a first server;

sending an enrollment request from the user to the first server using the first secure connection;

encrypting the enrollment request at the first server and thereafter sending the encrypted enrollment request to a host application;

sending encrypted enrollment information from the host application to the first server, the enrollment information comprising a customer applet, a public key, a serial number and an account number, wherein the information is used for enrolling and selecting the access code by the user;

decrypting the customer applet at the first server and thereafter sending the customer applet over the first secure connection to the user;

establishing a second secure connection from the user to a second server using the customer applet;

selecting the access code by;

encrypting the access code with the public key using the customer applet;

linking the encrypted access code with the account number and the serial number from the first server and thereafter sending the linked data to the second server;

encrypting the linked data at the second server and thereafter sending the encrypted linked data to the host application;

verifying the account number and the serial number at the host application and thereafter creating authentication data;

encrypting the authentication data and the access code;

sending the encrypted authentication data and access code from the host application to the second server;

sending the encrypted authentication data and access code from the second server to the customer applet using the second secure connection; and

storing the encrypted authentication data and access code.

15. The method of claim 14, wherein storing the encrypted authentication data and access code includes storing at least a portion of the authentication data and the access code in the customer applet.

16. The method of claim 14, wherein storing the encrypted authentication data and access code includes storing at least a portion of the authentication data and the access code on a mobile storage medium.

17. The method of claim 16, wherein the mobile storage medium is a smart card device which may be used to access an account from at least one remote location.

18. A system for providing and authenticating an access code over a network, comprising:

a user device;

a first server, coupled to the user device, for encrypting and decrypting enrollment information, the information comprising an enrollment request and an enrollment applet;

a second server, coupled to the user device, for encrypting and decrypting authorization information, the authorization information comprising an access code and authentication data;

a host application, coupled to the first server and the second server, for verifying and transmitting authorization information and enrollment information;

a first secure connection for coupling the first server and the user device;

a second secure connection for coupling the second server and the user device; and

a customer applet, transmitted from the host application to the user device over the first secure connection, for allowing a user to enter enrollment information comprising an access code.

19. The system of claim 18, wherein the first and second secure connections are SSL connections.

20. The system of claim 18, wherein the customer applet establishes the second secure connection in response to a user entering enrollment information.

21. The system of claim 18, further comprising a plurality of hardware service modules, one each coupled to the first server, the second server and the host application, for performing cryptography.

22. The system of claim 18, wherein the user device comprises a personal digital assistant.

23. The system of claim 18, wherein the user device comprises a personal computer.

24. The system of claim 18, wherein at least a portion of the customer applet is stored on a smart card device, wherein the smart card device may be used to access an account from at least one remote location.

25. The system of claim 18, wherein the access code is a personal identification number (PIN).

26. The system of claim 18, wherein the access code is a password.

"Express Mail" 27 Sep 2001